

**Amendments to the Specification:**

*Please replace the paragraph spanning lines 1-17 on page 6 with the following amended paragraph:*

In order to allow the PC 10 to use the mobile phone 30 as a CSP, there must obviously be a communication link between them. The connection may be wired, or wireless. Advantageously, communications between the personal computer 10 and mobile phone 30 can take place using the Bluetooth short-range radio transmission protocol, although an infrared connection is also possible. Regardless of whether a wired, or wireless connection is used, those aspects of the connection residing within the mobile phone 30 constitute means for connection to the PC 10 (which is external, and therefore remote from, the mobile phone 30) without involving the wireless communications network that the mobile phone 30 is additionally capable of communicating with. The protocol for the connection can for example be based on AT commands, and provides security for those communications. The command set is advantageously a version of the command set defined in a standard such as PKCS#11, described in the document "PKCS#11 v2.10: Cryptographic Token Interface Standard", published by RSA Security Inc. and incorporated herein by reference, where the commands are redefined as AT commands.

*Please replace the paragraph spanning lines 20-22 on page 8 with the following amended paragraph:*

Then, in step 138, the result of the cryptographic operation is sent back to the PC over the previously established communication link. It will thus be recognized that, as the previously established communication link between the MS 30 and the PC 10 is used for this communication, the MS 30 therefore functions as a cryptographic service provider to the PC 10 for encrypting communications from the PC 10 over the network 12 without the MS 30 sending the encrypted communications over the wireless communications network with which the MS 30 can also communicate.

*Please substitute the following amended paragraph for the paragraph spanning line 30 on page 10 through line 10 on page 11:*

In order to allow the PC 60 to use the mobile phone 30 as a CSP, there is a communication link between them. As in other embodiments of the invention, the connection may be wired, or wireless. Advantageously, communications between the personal computer 60 and mobile phone 30 can take place using the Bluetooth short-range radio transmission protocol, although an infrared connection is also possible. Regardless of whether a wired, or wireless connection is used, those aspects of the connection residing within the mobile phone 30 constitute means for connection to the PC 60 (which is external, and therefore remote from, the mobile phone 30) without involving the wireless communications network that the mobile phone 30 is additionally capable of communicating with. The protocol for the connection can for example be based on AT commands, and provides security for those communications. The command set is advantageously a version of the command set defined in a standard such as PKCS#11, described in the document "PKCS#11 v2.10: Cryptographic Token Interface Standard", published by RSA Security Inc. and incorporated herein by reference, where the commands are redefined as AT commands.

*Please replace the paragraph spanning lines 5-8 on page 12 with the following amended paragraph:*

In step 170, the result of the operation in the MS 30 is sent to the CT\* 26, which then responds to the application which requested the cryptographic functionality. It will thus be recognized that, as the previously established communication link between the MS 30 and the PC 60 is used for this communication, the MS 30 therefore functions as a cryptographic service provider to the PC 60 performing the requested cryptographic service and returning the results to the PC 60 without the MS 30 sending the encrypted communications over the wireless communications network with which the MS 30 can also communicate.